

A Note on a Conjecture for Balanced Elementary Symmetric Boolean Functions

Wei Su, Xiaohu Tang, and Alexander Pott

Abstract

In 2008, Cusick *et al.* conjectured that certain elementary symmetric Boolean functions of the form $\sigma_{2^{t+1}l-1, 2^t}$ are the only nonlinear balanced ones, where t, l are any positive integers, and $\sigma_{n,d} = \bigoplus_{1 \leq i_1 < \dots < i_d \leq n} x_{i_1} x_{i_2} \dots x_{i_d}$ for positive integers $n, 1 \leq d \leq n$. In this note, by analyzing the weight of $\sigma_{n, 2^t}$ and $\sigma_{n,d}$, we prove that $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ holds in most cases, and so does the conjecture. According to the remainder of modulo 4, we also consider the weight of $\sigma_{n,d}$ from two aspects: $n \equiv 3 \pmod{4}$ and $n \not\equiv 3 \pmod{4}$. Thus, we can simplify the conjecture. In particular, our results cover the most known results. In order to fully solve the conjecture, we also consider the weight of $\sigma_{n, 2^t+2^s}$ and give some experiment results on it.

Index Terms

Balancedness, algebraic degree, Boolean functions, elementary symmetric Boolean functions.

I. INTRODUCTION

Boolean functions are frequently used in the design of stream ciphers, block ciphers and hash functions. One of the most vital roles in cryptography of Boolean functions is to be used as filter and combination generators of stream ciphers based on linear feedback shift registers (LFSRs). Among all the Boolean functions, symmetric Boolean functions are an interesting subclass for their advantage in both implementation complexity and storage space.

Symmetric Boolean functions are characterized by the fact that their outputs only depend on the Hamming weights of their inputs. These functions can be represented in a very compact way both for their algebraic normal forms and for their value vectors, which considerably reduces the amount of memory required for storing the function and is of great interest in software applications. Elementary symmetric Boolean function is the basic unit composing of symmetric Boolean functions. Some cryptographically significant properties of (elementary) symmetric Boolean functions have been studied in [1]-[13].

Balancedness is the compulsory property for a Boolean function, since our cryptographic primitives is necessary to be unbiased in output. Recently, there are some results about the balancedness of elementary symmetric

W. Su is with the Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, 610031, China, and also with the Institute for Algebra and Geometry (IAG), Otto-von-Guericke University Magdeburg, D-39106 Magdeburg, Germany (e-mail: weisu0109@goosemail.com).

X. Tang is with the Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, 610031, China (e-mail: xhutang@ieee.org).

A. Pott is with the Institute for Algebra and Geometry (IAG), Otto-von-Guericke University Magdeburg, D-39106 Magdeburg, Germany (e-mail: alexander.pott@ovgu.de).

Boolean function $\sigma_{n,d}$:

$$\sigma_{n,d} = \bigoplus_{1 \leq i_1 < i_2 < \dots < i_d \leq n} x_{i_1} x_{i_2} \dots x_{i_d},$$

for $2 \leq d \leq n$.

In [8], Cusick *et al.* proved that $\sigma_{2^{t+1}l-1, 2^t}$ is balanced if t and l are positive integers (Theorem 3). Further, they presented the following conjecture.

Conjecture 1: There are no nonlinear balanced elementary symmetric Boolean functions except for $\sigma_{2^{t+1}l-1, 2^t}$, where t and l are any positive integers.

Towards this conjecture, some results have been obtained in [9]-[13].

- 1) If $d > 1$ is odd, then $\sigma_{n,d}$ is not balanced (Lemma 3.11, [9]);
- 2) If $d = 2^t$, then $\sigma_{n,d}$ is balanced if and only if n has the form of $n = 2^{t+1}l - 1$, where t and l are any positive integers (Corollary 3.10 and Lemmas 3.1, 3.17, [9]);
- 3) Let $n = 2^{t+1}l - 1$ for some positive integers t, l . If d is even and $2^t < d < 2^{t+1}$, then $\sigma_{n,d}$ is not balanced (Corollary 3.10 and Lemmas 3.1, 3.13, [9]);
- 4) Let $n = 2^{t+2}l + r - 1$, where $t, l > 0$ and $0 \leq r \leq 2^{t+1}$. If d is even and $2^t < d \leq 2^{t+1} - 2$, then $\sigma_{n,d}$ is not balanced (Corollary 3.10 and Lemmas 3.1, 3.18, [9]). Error correctly, the authors claimed in [9] that this result holds for $0 \leq r < 2^{t+1} + 2^t$, but the proof only work for $0 \leq r \leq 2^{t+1}$. It will be explained in details in Remark 1;
- 5) If $n = 2^{t+1}l - 1$, l odd and $2^{t+1} \nmid d$, $\sigma_{n,d}$ is balanced if and only if $d = 2^k$, $1 \leq k \leq t$ (Theorems 1, 2, 3 [10]);
- 6) Conjecture 1 holds for sufficiently large n . In particular, if d is not a power of two, then $\sigma_{n,d}$ is not balanced for sufficiently large n (Remark 3 [11]);
- 7) Let $r = \lfloor \log_2 d \rfloor + 1$. For any n , $n > -2(\log_2 \cos(\frac{\pi}{2^r}))^{-1}$, all these nonlinear balanced elementary symmetric Boolean functions are of the form $\sigma_{2^{t+1}l-1, 2^t}$, where t and l are any positive integers (Theorem 3 [12]). This implies that Conjecture 1 is true for large enough n ;
- 8) Let $d = 2^{t+w}(1+2^1+\dots+2^s)$ and $n = 2^{t+w+1}(1+2^1+\dots+2^s) + 2^t q + m$, $m \in \{-1, 0\}$. If the nonnegative integers t, w, s, q satisfy certain conditions, then $\sigma_{n,d}$ is not balanced (see Theorems 1-4 in [13] for more details).

In this note, we first consider the weight of $\sigma_{n, 2^t}$. By applying the relationship between $\sigma_{n,d}$ and $\sigma_{n, 2^t}$, we prove that $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ holds in most cases. Especially, these results cover the results given in [9].

Next according to the remainder of modulo 4, we consider the weight of $\sigma_{n,d}$ from two aspects: $n \equiv 3 \pmod{4}$ and $n \not\equiv 3 \pmod{4}$. Most notably, our results cover the results in [10]. Further, we prove that if $n = 2^{t+1}l - 1$, $l \geq 3$ odd and $2^{t+1} \mid d$, $\sigma_{n,d}$ is not balanced for $\text{wt}(d) = 1$ or $2d \nmid n$, which is not available in [10]. For $n \not\equiv 3 \pmod{4}$, we get some similar results as that of $n \equiv 3 \pmod{4}$:

- 1) If $n \not\equiv 3 \pmod{4}$, then $\sigma_{n, 2^s}$ is not balanced, for any $1 \leq s \leq \lfloor \log_2 n \rfloor$;
- 2) If $n \not\equiv 3 \pmod{4}$, then n can be written as $n = 2^{t+1}l + r$, where $l \geq 1$ is odd, $t \geq 1$, and $r \in \{0, 1, 2\}$. Let $2 \leq d = 2^{t+1}d' + d'' \leq n$ with $\text{wt}(d) \geq 2$, $d' \geq 0$ and $0 \leq d'' < 2^{t+1}$. Then, $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ if one of the following conditions holds: a) $l = 1$; b) $l \geq 3$, $d'' = 0$, and $d' \not\equiv \frac{l-1}{2}$; c) $l \geq 3$, $d'' > 0$, and $(d' \not\equiv \frac{l-1}{2}$ or $d'' \neq 2^t)$.

Thus, Conjecture 1 can be simplified as follows.

Conjecture 2: Let $l \geq 3$ be odd, $t \geq 1$, $n = 2^{t+1}l + r$, $r = -1, 0, 1, 2$. The elementary symmetric Boolean function $\sigma_{n,d}$ is not balanced in the following cases:

- 1) $d = 2^{t+1}d'$, $\text{wt}(d') \geq 2$ and $2 \leq d' \leq \frac{l-1}{2}$ for $r = -1, 0, 1, 2$;
- 2) $d = 2^{t+1}d' + 2^t$, $1 \leq d' \leq \frac{l-1}{2}$ for $r = 0, 1, 2$.

Therefore, to show that Conjecture 1 is true, it suffices to prove Conjecture 2.

In [11] and [12], the results for Conjecture 1 hold when n is large enough. And the conclusions in [13] are only for very special n and d . Compared with those results, our results are different.

This note is organized as follows. Section II introduces the notation and the related results about Boolean functions and symmetric Boolean functions. In Section III, we give our main results about the weight of $\sigma_{n,2^t}$ and $\sigma_{n,d}$. We prove that $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ holds in most cases. In Section IV, we discuss the weight of $\sigma_{n,d}$ depending whether $n \equiv 3(\text{mod } 4)$ or $n \not\equiv 3(\text{mod } 4)$. And then Conjecture 1 can be simplified as Conjecture 2. In order to fully solve the conjecture, we also consider the weight of $\sigma_{n,2^t+2^s}$ and give some experiment results on $\text{wt}(\sigma_{n,2^t+2^s})$ in Section V.

II. PRELIMINARIES

Throughout this note, let \mathbb{F}_2 be the finite field with two elements, $n > 0$ be a positive integer, and \mathbb{F}_2^n be the n -dimensional vector space over \mathbb{F}_2 . To avoid confusion, we denote the sum over \mathbb{Z} by $+$, and the sum over \mathbb{F}_2 by \oplus .

We first recall some necessary definitions and results about Boolean functions and symmetric Boolean functions.

A. Boolean Functions

Let \mathcal{B}_n be the set of all maps from \mathbb{F}_2^n to \mathbb{F}_2 . Such a map is called an n -variable Boolean function. The *support* of a Boolean function $f \in \mathcal{B}_n$ is defined as $\text{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. The *Hamming weight* $\text{wt}(f)$ of f is the cardinality of $\text{supp}(f)$, i.e., $\text{wt}(f) = |\text{supp}(f)|$. The *Hamming weight* of a binary vector $u = (u_1, u_2, \dots, u_n) \in \mathbb{F}_2^n$, is defined by $\text{wt}(u) = \sum_{i=1}^n u_i$. We say that an n -variable Boolean function f is *balanced* if $\text{wt}(f) = 2^{n-1}$.

Each Boolean function $f(x_1, \dots, x_n)$ has a unique representation by a multivariate polynomial over \mathbb{F}_2 , called the *algebraic normal form (ANF)*:

$$f(x_1, \dots, x_n) = \bigoplus_{u=(u_1, u_2, \dots, u_n) \in \mathbb{F}_2^n} f_u \prod_{i=1}^n x_i^{u_i}, \quad f_u \in \mathbb{F}_2.$$

The *algebraic degree* of f , denoted by $\deg(f)$, is the maximal value of $\text{wt}(u)$ such that $f_u \neq 0$. A Boolean function is called *affine* if it has degree at most 1. Note that any nonconstant affine function is balanced.

B. Symmetric Boolean Functions

Definition 1: A Boolean function f is said to be *symmetric* if

$$f(x_1, \dots, x_n) = f(x_{\tau(1)}, \dots, x_{\tau(n)}),$$

for any permutation τ of $\{1, 2, \dots, n\}$.

Denote by \mathcal{SB}_n the set of all n -variable symmetric Boolean functions. The definition implies that a symmetric Boolean function f takes the same value for all the vectors with the same weight. Therefore every $f \in \mathcal{SB}_n$ can be simply represented by a vector

$$v_f = (v_f(0), v_f(1), \dots, v_f(n)) \in \mathbb{F}_2^{n+1},$$

where the component $v_f(i) = f(x)$ with $\text{wt}(x) = i$. The vector v_f is called the *simplified value vector* of f .

Definition 2: For positive integers n and d , $1 \leq d \leq n$, the *elementary symmetric Boolean function* $\sigma_{n,d}$ is defined as

$$\sigma_{n,d} = \bigoplus_{1 \leq i_1 < i_2 < \dots < i_d \leq n} x_{i_1} x_{i_2} \dots x_{i_d}.$$

Based on the elementary symmetric Boolean functions, the algebraic normal form of $f \in \mathcal{SB}_n$ can be simplified as follows:

$$f(x_1, \dots, x_n) = \bigoplus_{i=0}^n \lambda_f(i) \sigma_{n,i}, \quad \lambda_f(i) \in \mathbb{F}_2.$$

The coefficients vector $\lambda_f = (\lambda_f(0), \lambda_f(1), \dots, \lambda_f(n))$ is called the *simplified ANF vector* of f .

Let n and m be two positive integers with their 2-adic expansions $n = n_{k-1}2^{k-1} + \dots + n_12 + n_0$ and $m = m_{k-1}2^{k-1} + \dots + m_12 + m_0$ respectively. We say that $m \preceq n$ if $m_i \preceq n_i$ for all $0 \leq i < k$, and otherwise $m \not\preceq n$.

Lemma 1: (Lucas' formula) For non-negative integers n and m , the following congruence relation holds

$$\binom{n}{m} \equiv \prod_{i=0}^{k-1} \binom{n_i}{m_i} \pmod{2}.$$

Then, $\binom{n}{m} \equiv 1 \pmod{2}$ if and only if $m \preceq n$.

Lemma 2: ([6]) Let $f \in \mathcal{SB}_n$. Its simplified value vector v_f and simplified ANF vector λ_f are related by

$$v_f(i) = \bigoplus_{k \preceq i} \lambda_f(k) \text{ and } \lambda_f(i) = \bigoplus_{k \preceq i} v_f(k), \quad \forall i \in \{0, 1, \dots, n\}.$$

By Lemma 2, we have

$$v_{\sigma_{n,d}}(i) = 1 \text{ iff } d \preceq i. \quad (1)$$

Thus, the weight of elementary symmetric Boolean function $\sigma_{n,d}$ is

$$\text{wt}(\sigma_{n,d}) = \sum_{i=0}^n \binom{n}{i} v_{\sigma_{n,d}}(i) = \sum_{d \preceq i} \binom{n}{i}. \quad (2)$$

III. OUR MAIN RESULTS

In this section, we obtain our main results about the weight of $\sigma_{n,2^t}$ and $\sigma_{n,d}$. We first consider the weight of $\sigma_{n,2^t}$. Next analyzing the weight of $\sigma_{n,d}$, we prove that $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ holds in most cases. Most notably, we can easily interpret the results in [8], [9] by using these results.

Let n and L be two positive integers with $1 \leq L \leq n$. For $0 \leq i \leq L-1$, denote

$$A_n^L(i) = \sum_{0 \leq j \leq n, j \equiv i \pmod{L}} \binom{n}{j}.$$

Since $2^t \preceq i$ iff $i = 2^{t+1}i' + 2^t + q$ for some integers $i' \geq 0$ and q with $0 \leq q \leq 2^t - 1$, we have $i \equiv 2^t + q \pmod{2^{t+1}}$. It follows from (1) and (2) that

$$\text{wt}(\sigma_{n,2^t}) = A_n^{2^{t+1}}(2^t) + A_n^{2^{t+1}}(2^t + 1) + \cdots + A_n^{2^{t+1}}(2^{t+1} - 1). \quad (3)$$

There is an equation about $A_n^{2^p}(i)$ given by Canteaut and Videau in [6].

Lemma 3: ([6]) For positive integers n, p, i , we have

$$A_n^{2^p}(i) = 2^{n-p} + 2^{1-p} \sum_{j=1}^{2^{p-1}-1} (2 \cos \frac{j\pi}{2^p})^n \cos \frac{j(n-2i)\pi}{2^p}.$$

The following lemma will be very useful for our discussion on that the weight of $\sigma_{n,2^t}$ is greater than, less than or equal to 2^{n-1} .

Lemma 4: ([9]) Let t and r be two positive integers. Suppose that $a_1 \geq a_3 \geq a_5 \geq \cdots \geq a_J$, with $J = 2K + 1$, are nonnegative integers. Define the sum

$$T = \sum_{1 \leq j \leq J, j \text{ odd}} a_j \sin \frac{j r \pi}{2^{t+1}}.$$

Then T has the same sign as $\sin \frac{r\pi}{2^{t+1}}$.

With all the above preparation, we can consider the weight of $\sigma_{n,2^t}$. Consequently, we obtain the following results.

Theorem 1: Let t be a positive integer and $d = 2^t$. For any positive integer $n \geq d$, n can be written as $n = 2^{t+2}l + r$ for some integers $l \geq 0$ and $0 \leq r \leq 2^{t+2} - 1$. Then we have

$$\text{wt}(\sigma_{n,d}) \begin{cases} < 2^{n-1}, & \text{if } 0 \leq r \leq 2^{t+1} - 2, \\ = 2^{n-1}, & \text{if } r = 2^{t+1} - 1 \text{ or } 2^{t+2} - 1, \\ > 2^{n-1}, & \text{if } 2^{t+1} \leq r \leq 2^{t+2} - 2. \end{cases}$$

Proof: Applying Lemma 3 to (3) in place of $p = t + 1$, one has

$$\begin{aligned} \text{wt}(\sigma_{n,2^t}) &= A_n^{2^{t+1}}(2^t) + A_n^{2^{t+1}}(2^t + 1) + \cdots + A_n^{2^{t+1}}(2^{t+1} - 1) \\ &= \sum_{i=2^t}^{2^{t+1}-1} [2^{n-(t+1)} + 2^{-t} \sum_{j=1}^{2^t-1} (2 \cos \frac{j\pi}{2^{t+1}})^n \cos \frac{j(n-2i)\pi}{2^{t+1}}] \\ &= 2^{n-1} + 2^{n-t} \sum_{j=1}^{2^t-1} (\cos \frac{j\pi}{2^{t+1}})^n \sum_{i=2^t}^{2^{t+1}-1} \cos \frac{j(n-2i)\pi}{2^{t+1}}. \end{aligned}$$

From the formula in [14]:

$$\sum_{s=0}^N \cos(sx + y) = \csc \frac{x}{2} \cos(\frac{Nx}{2} + y) \sin \frac{(N+1)x}{2}, \quad (4)$$

one gets

$$\begin{aligned}
\sum_{i=2^t}^{2^{t+1}-1} \cos \frac{j(n-2i)\pi}{2^{t+1}} &= \sum_{i=0}^{2^t-1} \cos \frac{j(n-2i-2^{t+1})\pi}{2^{t+1}} \\
&= (-1)^j \sum_{i=0}^{2^t-1} \cos \frac{j(n-2i)\pi}{2^{t+1}} \\
&= (-1)^j \sum_{i=0}^{2^t-1} \cos \frac{j(2^{t+2}l+r-2i)\pi}{2^{t+1}} \\
&= (-1)^j \sum_{i=0}^{2^t-1} \cos \frac{j(r-2i)\pi}{2^{t+1}} \\
&= (-1)^j \csc\left(-\frac{j\pi}{2^{t+1}}\right) \cos\left(-\frac{(2^t-1)j\pi}{2^{t+1}} + \frac{jr\pi}{2^{t+1}}\right) \sin\left(-\frac{2^t j\pi}{2^{t+1}}\right) \\
&= (-1)^j \csc \frac{j\pi}{2^{t+1}} \cos\left(-\frac{j\pi}{2} + \frac{j(r+1)\pi}{2^{t+1}}\right) \sin \frac{j\pi}{2} \\
&= \begin{cases} 0, & \text{if } j \text{ is even,} \\ -\csc \frac{j\pi}{2^{t+1}} \sin \frac{j(r+1)\pi}{2^{t+1}}, & \text{if } j \text{ is odd.} \end{cases}
\end{aligned}$$

Thus,

$$\text{wt}(\sigma_{n,2^t}) = 2^{n-1} - 2^{n-t} \sum_{1 \leq j \leq 2^t-1, j \text{ odd}} (\cos \frac{j\pi}{2^{t+1}})^n \csc \frac{j\pi}{2^{t+1}} \sin \frac{j(r+1)\pi}{2^{t+1}}.$$

Let $a_j = (\cos \frac{j\pi}{2^{t+1}})^n \csc \frac{j\pi}{2^{t+1}}$, $1 \leq j \leq 2^t - 1$. Then $a_1 > a_2 > \dots > a_{2^t-1} > 0$. Denote

$$T = \sum_{1 \leq j \leq 2^t-1, j \text{ odd}} (\cos \frac{j\pi}{2^{t+1}})^n \csc \frac{j\pi}{2^{t+1}} \sin \frac{j(r+1)\pi}{2^{t+1}} = \sum_{1 \leq j \leq 2^t-1, j \text{ odd}} a_j \sin \frac{j(r+1)\pi}{2^{t+1}}.$$

By Lemma 4, T has the same sign as $\sin \frac{(r+1)\pi}{2^{t+1}}$. Since

$$\sin \frac{(r+1)\pi}{2^{t+1}} \begin{cases} > 0, & \text{if } 0 \leq r \leq 2^{t+1} - 2, \\ = 0, & \text{if } r = 2^{t+1} - 1 \text{ or } 2^{t+2} - 1, \\ < 0, & \text{if } 2^{t+1} \leq r \leq 2^{t+2} - 2, \end{cases}$$

and $\text{wt}(\sigma_{n,2^t}) = 2^{n-1} - 2^{n-t}T$. The result holds. \square

By Theorem 1, the following corollary in [9] is obvious.

Corollary 1: ([9]) Let n and t be two positive integers with $2^t \leq n$. Then $\sigma_{n,2^t}$ is balanced if and only if n can be written as $n = 2^{t+1}l - 1$ for some positive integer l .

Let $i = \sum_{k=0}^m i_k 2^k$ and $j = \sum_{k=0}^m j_k 2^k$ with $i_k, j_k \in \mathbb{F}_2$. Define operation \vee :

$$i \vee j = \sum_{k=0}^m \max\{i_k, j_k\} 2^k.$$

Denote $\lfloor x \rfloor$ as the largest integer less than or equal to x . By equation (1), we have the following Lemma.

Lemma 5: [4] Let $m = \lfloor \log_2 n \rfloor$, $i = \sum_{k=0}^m i_k 2^k$ and $j = \sum_{k=0}^m j_k 2^k$ with $i_k, j_k \in \mathbb{F}_2$. Then we have

- 1) $\sigma_{n,j} = \sigma_{n,1}^{j_0} \sigma_{n,2}^{j_1} \sigma_{n,2^2}^{j_2} \dots \sigma_{n,2^m}^{j_m}$;
- 2) $\sigma_{n,i} \sigma_{n,j} = \sigma_{n,i \vee j}$.

Based on Theorem 1 and Lemma 5, we can get the following three corollaries about $\text{wt}(\sigma_{n,d})$ with $\text{wt}(d) \geq 2$.

Corollary 2: Let n, d be two positive integers with $d = 2^{d_1} + 2^{d_2} + \dots + 2^{d_s}$, $s \geq 2$ and $0 \leq d_1 < d_2 < \dots < d_s \leq \lfloor \log_2 n \rfloor$. If there exists $1 \leq i \leq s$, such that $\text{wt}(\sigma_{n,2^{d_i}}) \leq 2^{n-1}$. Then $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

Proof: Using Lemma 5, we have

$$\sigma_{n,d} = \sigma_{n,2^{d_1}} \sigma_{n,2^{d_2}} \cdots \sigma_{n,2^{d_s}}.$$

For any $0 \leq k \leq n$, one has that

$$v_{\sigma_{n,d}}(k) = 1 \iff v_{\sigma_{n,2^{d_j}}}(k) = 1, \quad \forall 1 \leq j \leq s,$$

which implies $\text{supp}(\sigma_{n,d}) \subseteq \text{supp}(\sigma_{n,2^{d_j}})$ for any $1 \leq j \leq s$. But, $v_{\sigma_{n,2^{d_i}}}(2^{d_i}) = 1$, $v_{\sigma_{n,2^{d_j}}}(2^{d_i}) = 0$ for $j \neq i$, and then $v_{\sigma_{n,d}}(2^{d_i}) = 0$. Thus, $\text{supp}(\sigma_{n,d}) \subset \text{supp}(\sigma_{n,2^{d_i}})$ and

$$\text{wt}(\sigma_{n,d}) < \text{wt}(\sigma_{n,2^{d_i}}) \leq 2^{n-1}.$$

□

Corollary 3: Let n, d be two positive integers with $d > 1$ being odd. Then $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

Proof: If $d > 1$ is odd, then $d = 1 + d'$, where $d' \geq 2$ is even. By applying Lemma 5-2), one has $\sigma_{n,d} = \sigma_{n,1} \sigma_{n,d'}$. Clearly, $\text{wt}(\sigma_{n,1}) = 2^{n-1}$ since $\sigma_{n,1}$ is a linear function and then is balanced. It follows from Corollary 2 that $\text{wt}(\sigma_{n,d}) < 2^{n-1}$. □

Corollary 4: Let n, d be two positive integers with $d = 2^{d_1} + 2^{d_2} + \dots + 2^{d_s}$, $s \geq 2$ and $1 \leq d_1 < d_2 < \dots < d_s \leq \lfloor \log_2 n \rfloor$. If $2d \not\leq n$ or $2^{d_1+2} - 1 \leq n$, then $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

Proof: According to Theorem 1, $\text{wt}(\sigma_{n,2^t}) \leq 2^{n-1}$ if and only if $n \equiv r \pmod{2^{t+2}}$, where $0 \leq r \leq 2^{t+1} - 1$ or $r = 2^{t+2} - 1$. That is $2^{t+1} \not\leq n$ or $2^{t+2} - 1 \leq n$. Combined with Corollary 2, if there exists $1 \leq i \leq s$, such that $2^{d_i+1} \not\leq n$ or $2^{d_i+2} - 1 \leq n$, then $\text{wt}(\sigma_{n,d}) < 2^{n-1}$. Since $2^{d_1+2} - 1 \leq 2^{d_i+2} - 1$ for any $1 \leq i \leq s$, we have

$$2^{d_i+2} - 1 \leq n \text{ for some } 1 \leq i \leq s \iff 2^{d_1+2} - 1 \leq n.$$

Obviously, $2^{d_i+1} \not\leq n$ for some $1 \leq i \leq s$ iff $2d \not\leq n$. This completes the proof. □

By the above results, we can obtain that $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ holds in most cases, and so does the conjecture.

Remark 1: Learned from the authors of [9] we knew that the result given in Lemma 3.18 [9] holds for $0 \leq r \leq 2^{t+1}$ instead for $0 \leq r < 2^{t+1} + 2^t$.

If d' is odd and $2^t + 1 < d' \leq 2^{t+1} - 1$ for some positive integer t . Let $n' = 2^{t+1} \cdot l' + r$. Since $2^t + 1 \leq d'$ and $2^t + 1 \neq d'$, by Lemma 5, one has $\text{wt}(\sigma_{n',d'}) < \text{wt}(\sigma_{n',2^{t+1}})$. Since

$$\text{wt}(\sigma_{n',2^{t+1}}) = \sum_{s=0}^{2^{t-1}-1} A_{n'}^{2^{t+1}}(2^t + 2s + 1) = 2^{n'-2} + 2^{n'-t-1}(-1)^{l'+1} \sum_{j=1, \text{odd}}^{2^t-1} \left(\cos \frac{j\pi}{2^{t+1}}\right)^{n'-1} \frac{\sin \frac{jr\pi}{2^{t+1}}}{\sin \frac{j\pi}{2^{t+1}}}.$$

- 1) If $r = 0$ or 2^{t+1} , then $\text{wt}(\sigma_{n',2^{t+1}}) = 2^{n'-2}$;
- 2) If $1 \leq r < 2^{t+1}$, then $\sin(\frac{r\pi}{2^{t+1}}) > 0$. Since $\frac{(\cos \frac{j\pi}{2^{t+1}})^{n'-1}}{\sin \frac{j\pi}{2^{t+1}}}$ strictly decreases as j increases for $1 \leq j \leq 2^t - 1$, by Lemma 4, one has $\text{wt}(\sigma_{n',2^{t+1}}) < 2^{n'-2}$ if l' is even;
- 3) Similarly, if l' is even and $2^{t+1} < r < 2^{t+1} + 2^t$, then $\text{wt}(\sigma_{n',2^{t+1}}) > 2^{n'-2}$.

Thus, we can only obtain that $\text{wt}(\sigma_{n',d'}) \neq 2^{n'-2}$ for even l' and $0 \leq r \leq 2^{t+1}$.

Remark 2: The above results cover the known results in [8], [9].

- 1) It has been proved that if $\sigma_{n,d}$ is balanced, then $d \leq \lceil \frac{n}{2} \rceil$ [8]. In fact, if $\text{wt}(d) \geq 2$ and $\sigma_{n,d}$ is balanced, by Corollaries 3 and 4, one has d must be even and $2d \leq n$. Thus, $d \leq \lfloor \frac{n}{2} \rfloor$.

- 2) Let $n = 2^{t+1}l - 1$ for some positive integers t, l . If d is even and $2^t < d < 2^{t+1}$, then d can be written as $d = 2^{d_1} + 2^{d_2} + \dots + 2^{d_{s-1}} + 2^t$, where $s \geq 2$ and $1 \leq d_1 < d_2 < \dots < d_{s-1} < t$. Thus, $d_1 + 2 \leq t + 1$ and $2^{d_1+2} - 1 \preceq 2^{t+1} - 1 \preceq n$. By Corollary 4, one has $\text{wt}(\sigma_{n,d}) < 2^{n-1}$. So the result obtained by Corollary 3.10 and Lemmas 3.1, 3.13 in [9] is a special case of Corollary 4;
- 3) Let $n = 2^{t+2}l + r - 1$ for some positive integers t, l and $0 \leq r \leq 2^{t+1}$. If d is even and $2^t < d < 2^{t+1}$, then $\sigma_{n,d}$ is not balanced. The proof is as follows.
- a) If $r = 0$, then $n = 2^{t+2}l - 1$. It is a special case of 2), and so a special case of Corollary 4;
- b) If $1 \leq r \leq 2^{t+1}$. Since d is even and $2^t < d < 2^{t+1}$, $d = 2^t + d'$ for some even integer $2 \leq d' \leq 2^t - 2$. Then, $2d = 2^{t+1} + 2d' \not\preceq n$. By Corollary 4, one has $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

Thus, the result obtained by Corollary 3.10, Lemmas 3.1, and the modified Lemma 3.18 in [9] (replace $0 \leq r < 2^{t+1} + 2^t$ with $0 \leq r \leq 2^{t+1}$) is also a special case of Corollary 4.

IV. THE WEIGHT OF $\sigma_{n,d}$

In the section, we will discuss the weight of $\sigma_{n,d}$ depending whether $n \equiv 3(\text{mod } 4)$ or $n \not\equiv 3(\text{mod } 4)$. If $n \equiv 3(\text{mod } 4)$, our results cover the results in [10]. Furthermore, if $n = 2^{t+1}l - 1$, $l \geq 3$ odd and $2^{t+1} \nmid d$, then $\sigma_{n,d}$ is not balanced for $\text{wt}(d) = 1$ or $2d \not\preceq n$, which is not contained in [10]. We can also get results for $n \not\equiv 3(\text{mod } 4)$. As a result, Conjecture 1 can be simplified to Conjecture 2.

A. The Weight of $\sigma_{n,d}$ with $n \equiv 3(\text{mod } 4)$

When $n \geq 3$ and $n \equiv 3(\text{mod } 4)$, it can be written as $n = 2^{t+1}l - 1$, where $l \geq 1$ is odd and $t \geq 1$. For $\text{wt}(d) = 1$ and $\text{wt}(d) \geq 2$, we can obtain the following theorems, respectively. These results cover the results in [10].

Theorem 2: Let $n = 2^{t+1}l - 1$ and $d = 2^s$, where $l \geq 1$ is odd, $t \geq 1$ and $s \geq 1$. Then $\sigma_{n,d}$ is balanced if and only if $1 \leq s \leq t$.

Proof: By Corollary 1, $\sigma_{n,2^s}$ is balanced if and only if there exists $l' \geq 1$ such that $n = 2^{s+1}l' - 1$. For any given positive integers t, s , and odd l , there exists $l' \geq 1$ such that $2^{t+1}l - 1 = 2^{s+1}l' - 1$ if and only if $1 \leq s \leq t$. This finishes the proof. \square

If $d > 1$ is odd, by Corollary 3, we have $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

If d is even and $\text{wt}(d) \geq 2$, we have the following theorem.

Theorem 3: Let $n = 2^{t+1}l - 1$ and $2 \leq d = 2^{t+1}d' + d'' \leq n$, where $l \geq 1$ is odd, $t \geq 1$, $d' \geq 0$ and $0 \leq d'' < 2^{t+1}$. If d is even and $\text{wt}(d) \geq 2$, then $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ if one of the following conditions hold:

- 1) $l = 1$;
- 2) $l \geq 3$, $d'' > 0$;
- 3) $l \geq 3$, $d'' = 0$, and $d' \not\preceq \frac{l-1}{2}$.

Proof: Since l is odd, write it as $l = 2c + 1$, $c = \frac{l-1}{2} \geq 0$. Then $n = 2^{t+1}l - 1 = 2^{t+2}c + 2^{t+1} - 1$. If d is even and $\text{wt}(d) \geq 2$, then d can be written as $d = 2^{d_1} + 2^{d_2} + \dots + 2^{d_s}$ with $s \geq 2$ and $1 \leq d_1 < d_2 < \dots < d_s \leq \lfloor \log_2 n \rfloor$.

- 1) If $l = 1$, $n = 2^{t+1} - 1$. Since $1 \leq d_1 < d_s \leq t$, we have $d_1 + 2 \leq t + 1$ and $2^{d_1+2} - 1 \preceq n$. By Corollary 4, we obtain $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.
- 2) If $l \geq 3$ and $d'' > 0$, then $d'' = 2^{d_1} + 2^{d_2} + \dots + 2^{d_i}$ for some $1 \leq i \leq s$. Since $d'' < 2^{t+1}$, one has $1 \leq d_1 \leq t$. By Corollary 2, we get $\text{wt}(\sigma_{n,2^{d_1}}) = 2^{n-1}$. According to Corollary 2, $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

3) When $l \geq 3$ and $d'' = 0$. If $d' \not\leq c$, we have $2d = 2^{t+2}d' \not\leq n$. By Corollary 4, we have $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

The proof is completed. \square

In [10], the authors proved that if $n = 2^{t+1}l - 1$, l odd and $2^{t+1} \nmid d$, $\sigma_{n,d}$ is balanced if and only if $d = 2^k$, $1 \leq k \leq t$. Thus, the results in Corollary 3 and Theorems 2, 3 cover the results given in [10]. Furthermore, the result for $l \geq 3$ odd and $2^{t+1} \mid d$ is not contained in [10].

B. The Weight of $\sigma_{n,d}$ with $n \not\equiv 3 \pmod{4}$

When $n \geq 3$ and $n \not\equiv 3 \pmod{4}$, it can be written as $n = 2^{t+1}l + r$, where $l \geq 1$ is odd, $t \geq 1$, and $r = 0, 1, 2$. Similarly, we have the following results.

Theorem 4: Let $n \geq 3$ and $d = 2^s \leq n$ with $s \geq 1$. If $n \not\equiv 3 \pmod{4}$, then the elementary symmetric Boolean function $\sigma_{n,d}$ is not balanced.

Proof: The result directly follows from Corollary 1. \square

If $d > 1$ is odd, by Corollary 3, we have $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

If d is even and $\text{wt}(d) \geq 2$, we have the following result.

Theorem 5: Let $n = 2^{t+1}l + r$ and $2 \leq d = 2^{t+1}d' + d'' \leq n$ with $l \geq 1$ is odd, $t \geq 1$, $r \in \{0, 1, 2\}$, $d' \geq 0$, and $0 \leq d'' < 2^{t+1}$. If d is even and $\text{wt}(d) \geq 2$. Then, $\text{wt}(\sigma_{n,d}) < 2^{n-1}$ if one of the following conditions holds:

- 1) $l = 1$;
- 2) $l \geq 3$, $d'' = 0$, and $d' \not\leq \frac{l-1}{2}$;
- 3) $l \geq 3$, $d'' > 0$, and $(d' \not\leq \frac{l-1}{2} \text{ or } d'' \neq 2^t)$.

Proof: Since l is odd, write it as $l = 2c + 1$, $c = \frac{l-1}{2} \geq 0$. Then $n = 2^{t+1}l + r = 2^{t+2}c + 2^{t+1} + r$.

- 1) When $l = 1$, $n = 2^{t+1} + r$. Since d is even, $\text{wt}(d) \geq 2$, one has $4 \mid 2d$ and $\text{wt}(2d) \geq 2$. Thus, $2d \not\leq n$. By Corollary 4, we obtain $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.
- 2) When $l \geq 3$ and $d'' = 0$. If $d' \not\leq c$, we have $2^{t+2}d' \not\leq 2^{t+2}c + 2^{t+1} + r$. That is, $2d \not\leq n$. By Corollary 4, we obtain $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.
- 3) When $l \geq 3$ and $d'' > 0$. Since d is even, one has $d'' \geq 2$ and $4 \mid 2d''$. Therefore, $2d'' \not\equiv 2^{t+1} + 1 \pmod{2^{t+2}}$ and $2d'' \not\equiv 2^{t+1} + 2 \pmod{2^{t+2}}$.

If $d'' \neq 2^t$, then $2d'' \not\equiv 2^{t+1} \pmod{2^{t+2}}$. So, $2d'' \not\equiv 2^{t+1}, 2^{t+1} + 1, 2^{t+1} + 2 \pmod{2^{t+2}}$. From $2d'' \geq 4 > r$, one has $2d'' \not\equiv r, 2^{t+1}, 2^{t+1} + r \pmod{2^{t+2}}$. Thus, $2d'' \not\leq 2^{t+1} + r$ and $2d \not\leq n$. If $d' \not\leq c$, we also have $2d \not\leq n$. By Corollary 4, we get $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

The proof is completed. \square

From Corollary 3 and Theorems 2-5, Conjecture 1 holds in most cases and the unsolved conditions are

- 1) $d = 2^{t+1}d'$, $\text{wt}(d') \geq 2$ and $2 \leq d' \leq \frac{l-1}{2}$ for $r = -1, 0, 1, 2$; Or
- 2) $d = 2^{t+1}d' + 2^t$, $1 \leq d' \leq \frac{l-1}{2}$ for $r = 0, 1, 2$,

where $n = 2^{t+1}l + r$, $l \geq 3$ is odd, and $t \geq 1$.

Thus, Conjecture 1 can be simplified as Conjecture 2.

V. THE WEIGHT OF $\sigma_{n,2^t+2^s}$

In order to solve the conjecture, we consider the weight of $\sigma_{n,2^t+2^s}$ and give some experiment results on $\text{wt}(\sigma_{n,2^t+2^s})$ in this section.

Theorem 6: Let n, d be two positive integers with $d = 2^t + 2^s \leq n$ and $1 \leq t < s \leq \lfloor \log_2 n \rfloor$. Then

$$\text{wt}(\sigma_{n,d}) = 2^{n-2} - 2^{n-s} \sum_{j=1, j \text{ odd}}^{2^s-1} (\cos a_j)^n \frac{\sin(2^t a_j) \sin((n-2^t+1)a_j)}{\sin(a_j) \sin(2^{t+1} a_j)}.$$

where $a_j = \frac{j\pi}{2^{s+1}}$.

Proof: Since $d \preceq i$ if and only if $i = 2^{s+1}i' + 2^s + 2^{t+1}p + 2^t + q$ for some non-negative integers i', p, q with $0 \leq p \leq 2^{s-t-1} - 1$ and $0 \leq q \leq 2^t - 1$. Thus, $i \equiv 2^s + 2^{t+1}p + 2^t + q \pmod{2^{s+1}}$ and

$$\begin{aligned} \text{wt}(\sigma_{n,d}) &= \sum_{p=0}^{2^{s-t-1}-1} \sum_{q=0}^{2^t-1} A_n^{2^{s+1}}(2^s + 2^{t+1}p + 2^t + q) \\ &= \sum_{p=0}^{2^{s-t-1}-1} \sum_{q=0}^{2^t-1} [2^{n-s-1} + 2^{-s} \sum_{j=1}^{2^s-1} (2 \cos \frac{j\pi}{2^{s+1}})^n \cos \frac{j(n-2^{s+1}-2^{t+2}p-2^{t+1}-2q)\pi}{2^{s+1}}] \\ &= 2^{n-2} + 2^{n-s} \sum_{j=1}^{2^s-1} (\cos a_j)^n \sum_{p=0}^{2^{s-t-1}-1} \sum_{q=0}^{2^t-1} \cos((n-2^{s+1}-2^{t+2}p-2^{t+1}-2q)a_j) \\ &= 2^{n-2} + 2^{n-s} \sum_{j=1}^{2^s-1} (\cos a_j)^n \cdot S_j, \end{aligned}$$

where $a_j = \frac{j\pi}{2^{s+1}}$ and $S_j = \sum_{p=0}^{2^{s-t-1}-1} \sum_{q=0}^{2^t-1} \cos((n-2^{s+1}-2^{t+2}p-2^{t+1}-2q)a_j)$ for $1 \leq j \leq 2^s - 1$. By using the formula (4), we get

$$\begin{aligned} S_j &= \sum_{p=0}^{2^{s-t-1}-1} \csc(-a_j) \cos((n-2^{s+1}-2^{t+2}p-2^{t+1}-2^t+1)a_j) \sin(-2^t a_j) \\ &= \csc(a_j) \sin(2^t a_j) \sum_{p=0}^{2^{s-t-1}-1} \cos((n-2^{s+1}-2^{t+2}p-2^{t+1}-2^t+1)a_j) \\ &= \csc(a_j) \sin(2^t a_j) \csc(2^{t+1} a_j) \cos((n-2^{s+1}-2^s-2^t+1)a_j) \sin(2^s a_j) \\ &= \csc(a_j) \sin(2^t a_j) \csc(2^{t+1} a_j) \cos((n-2^t+1)a_j - \frac{3j\pi}{2}) \sin \frac{j\pi}{2} \\ &= \begin{cases} 0, & \text{if } j \text{ is even,} \\ -\csc(a_j) \sin(2^t a_j) \csc(2^{t+1} a_j) \sin((n-2^t+1)a_j), & \text{if } j \text{ is odd.} \end{cases} \end{aligned}$$

Therefore,

$$\text{wt}(\sigma_{n,d}) = 2^{n-2} - 2^{n-s} \sum_{j=1, j \text{ odd}}^{2^s-1} (\cos a_j)^n \frac{\sin(2^t a_j) \sin((n-2^t+1)a_j)}{\sin(a_j) \sin(2^{t+1} a_j)}.$$

□

By Theorem 6, we see that it is hard to determine whether $\text{wt}(\sigma_{n,2^t+2^s})$ is greater than or less than 2^{n-1} . With the help of a computer, we calculate $\text{wt}(\sigma_{n,2^t+2^s})$ and find that

- 1) if $t = 1$ and $3 \leq l \leq 181$, then $\text{wt}(\sigma_{n,2^t+2^s}) < 2^{n-1}$;
- 2) if $t = 2$ and $l = 3$, then $n = 24 + r$, $\text{wt}(\sigma_{n,12}) > 2^{n-1}$ and $\text{wt}(\sigma_{n,20}) < 2^{n-1}$;
- 3) if $t = 2$ and $5 \leq l \leq 121$, then $\text{wt}(\sigma_{n,2^t+2^s}) < 2^{n-1}$;
- 4) if $t \geq 3$, some of $\text{wt}(\sigma_{n,2^t+2^s})$ are greater than 2^{n-1} ;

where $1 \leq t < s \leq \lfloor \log_2 n \rfloor$, $n = 2^{t+1}l + r$, $l \geq 3$ is odd, and $r \in \{0, 1, 2\}$.

From Corollary 2, we have if $\text{wt}(\sigma_{n,2^t+2^s}) < 2^{n-1}$ and $2^t + 2^s \preceq d$, then $\text{wt}(\sigma_{n,d}) < 2^{n-1}$.

REFERENCES

- [1] P. Savicky, "On the bent Boolean functions that are symmetric," *Eur. J. Combin.*, vol. 15, pp. 407-410, 1994.
- [2] S. Maitra and P. Sarkar, "Maximum nonlinearity of symmetric Boolean functions on odd number of variables," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2626-2630, 2002.
- [3] C. Carlet, "On the degree, nonlinearity, algebraic thickness and nonnormality of Boolean function, with developments on symmetric functions," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2178-2185, 2004.
- [4] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions," *Lecture Notes in Computer Science*, vol. 3797, pp. 35-48, 2005.
- [5] T.W. Cusick and L. Yuan, " k -th order symmetric SAC Boolean functions and bisecting binomial coefficients," *Discr. Appl. Math.*, vol. 149, pp. 73-86, 2005.
- [6] A. Canteaut and M. Videau, "Symmetric Boolean functions," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2791-2811, 2005.
- [7] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes", Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering," *Cambridge University Press* (Peter Hammer and Yves Crama editors), pages 257-397, 2010.
- [8] T.W. Cusick, Y. Li, and P. Stănică, "Balanced symmetric Boolean functions over $GF(p)$," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1304-1307, 2008.
- [9] T.W. Cusick, Y. Li, and P. Stănică, "On a conjecture for balanced symmetric Boolean functions," *J. Math. Crypt.*, vol. 3, no. 4, pp. 273-290, 2009.
- [10] G.P. Gao, W.F. Liu, and X.Y. Zhang, "The degree of balanced elementary symmetric Boolean functions of $4k + 3$ variables," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4822-4825, 2011.
- [11] F.N. Castro and L.A. Medina, "Linear recurrences and asymptotic behavior of exponential sums of symmetric boolean functions," *The Electronic Journal of Combinatorics*, vol. 18, no. 2, P8, 2011.
- [12] Y.M. Guo, G.P. Gao, and Y.Q. Zhao, "Recent results on balanced symmetric Boolean functions (Online)," available: <http://eprint.iacr.org/2012/093>.
- [13] Z.H. Ou and Y.Q. Zhao, "Unbalanced elementary symmetric Boolean functions with the degree d and $\text{wt}(d) \geq 3$ (Online)," available: <http://eprint.iacr.org/2012/101>.
- [14] E.R. Hansen, *A Table of Series and Products*, Prentice-Hall, Englewood Cliffs, NJ, 1975.